

DECLARATION OF SPECIAL AGENT DAVID HARDING

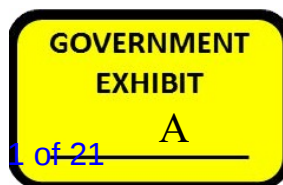
I, Special Agent David Harding with the Federal Bureau of Investigation assigned to the Charlotte, North Carolina Field Office with duty in the Raleigh Resident Agency, pursuant to 28 U.S.C. § 1746 and the laws of the United States, hereby declares under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

INTRODUCTION

1. This declaration is made in support of a complaint to forfeit funds previously seized from nine unhosted Tether cryptocurrency wallets. These wallets contained proceeds and/or comingled funds of a cryptocurrency investment fraud scheme, whereby one or more criminal fraudsters used a fraudulent cryptocurrency exchange to commit wire fraud by inducing victims known as K.W. and J.B. to send money to cryptocurrency wallets controlled by the fraudsters. Once they received the cryptocurrency, it was rapidly transferred to numerous other cryptocurrency wallets. The FBI previously obtained a seizure warrant pursuant to 18 U.S.C. § 981(b) to bring traceable proceeds and other comingled funds involved in money laundering into government custody and now submit this declaration to support the funds' forfeiture.

DECLARANT'S BACKGROUND AND EXPERIENCE

2. I am a Special Agent with the Federal Bureau of Investigation assigned to the Charlotte, North Carolina Field Office with duty in the Raleigh Resident Agency. I have been employed as a Special Agent with the FBI since 2012 and worked a variety of federal criminal investigations, including but not limited to complex financial crimes. This training included instruction in general law enforcement and criminal investigations to include violations of Title 18, United States Code, section 1343 (Wire Fraud) and section 1956 (money laundering).



3. In my official capacity as a Special Agent, I have obtained the information set forth in this declaration through personal knowledge and/or directly from persons having knowledge of the facts of this case, including, as relevant, from speaking with, or review of sources of information or other law enforcement personnel.

PURPOSE OF THE DECLARATION

4. I make this declaration in support of the civil forfeiture of the proceeds of a criminal scheme to defraud K.W. and J.B. executed in violation of 18 U.S.C. § 1343 and co-mingled funds that were involved in the unlawful laundering of such property in violation of 18 U.S.C. § 1956. Specifically, this declaration supports the civil forfeiture of the following assets contained in unhosted Tether wallets that were previously seized and brought into government custody on August 12, 2024. As part of the Tether-specific exemption to the MLAT requirement, Tether transferred all cryptocurrency totaling 4,992,845.06 USDT from the wallets to be seized to a new unhosted wallet before they transferred the cryptocurrency to an FBI created wallet. Tether then destroyed those seized wallets. Once that transfer to the FBI was complete, the entire proceeds were transferred to a wallet controlled by the U.S. Marshal Service pending forfeiture. The seized wallets and amounts are listed below:

	Seized Wallet Addresses	Amount Received (USDT)
a	0xF6438DeD9Eb47AAB9d41664664F201B498f905D6	500,000.00
b	0x6275Ca02c006E843b11FF9ea3c4d2a051a170e61	684,279.00
c	0x8b10c643D42374D63824a39932c3e66c5f07E3F4	500,000.00
d	0xc48436c1674EFcFe8fb8E96c3F6504324dD6D50e	500,000.00
e	0x1291bF41339300ebDBB4B289143b6d5f373ab553	500,000.05
f	0x06Ecb24C52C2d606d4F52ba9B7987002f0915CDc	500,000.00
g	0x874071288290361738Ea12Cd1389f4bcB4875eF3	500,000.00
h	0xD9B56f584EE14eA1Bc8712D0335fbb63E26AE693	999,742.01
i	0xDc35cE037722e2196a8B3eB9da64648Bc0E037C8	308,824.00
		<hr/> 4,992,845.06

5. As explained below, the foregoing funds represent directly traceable criminal proceeds and/or money involved in the laundering of those proceeds, which were derived from a criminal fraud scheme that successfully defrauded K.W. and J.B. by impersonating a legitimate cryptocurrency exchange and inducing K.W. and J.B. to transfer VC belonging to them to wallets in control of the fraudster(s).

BACKGROUND OF CRYPTOCURRENCY

6. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. *Cryptocurrency and Blockchain Generally*: Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Tether, USD Coin, and DAI. Each unit of cryptocurrency is often referred to as a “coin” or “token.” In general, most cryptocurrencies are considered fungible assets. For example, Bitcoin is considered fungible because each unit of Bitcoin is equivalent to any other unit, meaning they have the same quality and functionality. Regardless of when a unit of Bitcoin was issued (“mined”), all Bitcoin units are part of the same blockchain and have the same functionality. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Users of cryptocurrency use public and private keys to transfer cryptocurrency from one person or place to another. A public key is typically a set of numbers and/or letters that a cryptocurrency user shares with other users to engage in a transaction in cryptocurrency, whereas a private key is typically a set of numbers and/or letters that the user of an account maintains privately to access his or her cryptocurrency. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange,

or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. As such, most cryptocurrencies have a “blockchain,” which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.¹ Although many cryptocurrencies are or purport to be pseudonymous, often law enforcement and currency exchangers can use the blockchain to analyze transactions in cryptocurrency, identify individuals who are using cryptocurrency platforms for illicit purposes, and trace fraud proceeds from victims to one or more exchanges or wallets.

b. *Wallets*: Cryptocurrency is often stored in a virtual account called a wallet, which can exist in, among other forms, an external computer device, a computer, on an application, or online. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. Access to a wallet and the cryptocurrency therein is typically protected by a password only known to the owner or user of the wallet. Wallets can be either “custodial” or “non-custodial” (also referred to as “centralized/decentralized” or “hosted/non-hosted”). In the case of a non-custodial wallet, the owner of the wallet has sole control of the wallet’s private keys, which enable access to the wallet and any funds contained therein. With a custodial wallet, another party controls the private keys to the wallet. This is usually a cryptocurrency exchange, and the relationship between the exchange and the customer can be considered analogous to the relationship between a traditional bank and its customers, where the bank securely maintains funds deposited by a bank customer.

¹ Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

c. *Exchanges/Exchangers*: Virtual currency “exchangers” and “exchanges” (also referred to as a “Virtual Asset Service Provider” [VASP]), such as Binance, Coinbase, Kraken, and Crypto.com, are individuals or companies that exchange virtual currency for other currencies, including U.S. dollars. Exchanges facilitate the purchase, sale, and transfer of a variety of digital currencies.

d. *Centralized/Decentralized Exchanges*: Centralized exchanges generally maintain a custodial role for the wallets of its customers, and function as trusted intermediaries in cryptocurrency transactions. Decentralized exchanges consist of peer-to-peer marketplaces where users can trade cryptocurrencies in a non-custodial manner, without the need for an intermediary to facilitate the transfer and custody of funds. Decentralized exchanges are often used to trade, or “swap”, one type of cryptocurrency for another, for which the user pays a transaction fee. Centralized exchanges that conduct business in the United States are required to verify their customers’ identities and abide by Know-Your-Customer/Anti-Money Laundering (KYC/AML) regulations.

e. *Tether*: Tether, widely known as “USDT,” is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. dollars, making it what is known as a “stablecoin.” USDT is issued by Tether Ltd., a company headquartered in Hong Kong. Tether is connected to Bitfinex, a cryptocurrency exchange registered in the British Virgin Islands.

f. USDT is hosted on the Ethereum and Bitcoin blockchains, among others. Ethereum (“ETH”) is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses “smart contract” technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the

instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

g. Like other virtual currencies, USDT is sent to and received from USDT "addresses." A USDT address is somewhat analogous to a bank account number and is represented as a 26-to 35-character-long case-sensitive string of letters and numbers. Users can operate multiple USDT addresses at any given time, with the possibility of using a unique USDT address for every transaction. Although the identity of a USDT address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often be used to identify the owner of a particular USDT address. The analysis can also, in some instances, reveal additional addresses controlled by the same individual or entity. Unlike Bitcoin, one of the most popular cryptocurrencies in use today, USDT is "centralized", meaning that it is issued and controlled by a governing body. Most other cryptocurrencies are "decentralized" and have no such governing body.

FACTS SUPPORTING FORFEITURE

THE SCHEME

7. This case concerns a cryptocurrency investment fraud scam perpetrated on victims throughout the United States, including in the Eastern District of North Carolina. The scheme often begins when a fraudster sends a victim a seemingly innocuous and misdialled text message, or

through sending an unsolicited message to a victim's social media account. From there, the fraudster will attempt to establish a more personal relationship with the victim by using manipulative tactics similar to those used in online romance scams.

8. Once the fraudster has established a trusted relationship with the victim, the fraudster brings the victim into a cryptocurrency investment scheme. This fraudster typically claims to have a technique to quickly make large profits, either through personal expertise with cryptocurrency, or through a trusted relative or friend with insider information. The investment schemes have the appearance of a legitimate enterprise through the use of fabricated interfaces, derivative websites that appear related to legitimate companies, and other techniques designed to bolster the scheme's legitimacy. This generally includes a fake investment platform operated through a website or mobile application that displays a fictitious investment portfolio with abnormally large investment returns. The investment platforms are a ruse, and the funds contributed are routed directly to a cryptocurrency address the fraudsters control. In reality, the victims do not have actual "accounts" at the fake companies – as soon as the victim sends cryptocurrency to the deposit address provided by the fraudsters, it is immediately moved through many other wallets in order to launder the funds and make them harder to trace. The victims are able to see what they believe are their deposits on the fraudulent website, and the purported large returns on their investments are designed to convince them to invest more.

9. When the victims do attempt to withdraw their funds, they are unable to do so and are often met with various excuses, such as being told they are required to pay "taxes" or "penalties" in order to release their funds. The "tax" payments are an attempt by the scammers to elicit even more money out of the victims. The fraudsters, in the form of "customer service" for the fraudulent

website, will continue to ask for additional payments from the victim, and will not release the funds regardless of how much is paid.

10. In this case, multiple victims, one of whom (hereinafter “K.W.”) resides in the Eastern District of North Carolina, were victims of a cryptocurrency investment fraud scheme. This affidavit discusses two victims (“K.W.” and “J.B.”) of the same organization perpetrating the same investment fraud scheme. The victims were approached and recruited through the guise of a romantic relationship in order to develop a trusted relationship. Once the romantic relationship was established, the fraudster introduced K.W./J.B. to the fictitious trading platform, Bitkanant (the name of this trading platform is similar to a legitimate cryptocurrency trading platform, Bitkan). Based on an analysis of the fake investment platforms that all the victims were directed to, as well as tracing of the cryptocurrency that the victims sent, agents believe that the victims were all likely victimized by the same person or group. The following sections detail the background of one victim’s enticement into the scheme. This is followed by a section which demonstrates the link between the victims and shows that there are likely to be many more additional victims of the same group.

Victim K.W.

11. K.W. is 67 years old and a resident of Angier, North Carolina. In January 2023, a person claiming to be a woman named “Jeanie” contacted K.W. via text message and they began exchanging messages not related to investing or cryptocurrency. They later communicated via WhatsApp and Telegram. Jeanie (who later said her real name was Li Xueli) said she worked in fashion design in Miami, Florida. Jeanie also claimed to be from Hong Kong, with her mother being Chinese and her father being English. Jeanie provided multiple pictures of herself, some of which were later found associated with different names on various social media and websites, such

as LinkedIn. There are even screenshots of text communications with her picture attempting to engage other individuals.

12. Eventually the conversation turned to finances and investing. Jeanie claimed her uncle lived in Chicago, and he and his team developed an algorithm predicting the up-and-down price movement of Bitcoin and Ethereum on particular days at particular times. Jeanie then introduced K.W. to Bitkan, the legitimate international cryptocurrency exchange platform. But Jeanie provided K.W. the website link, Bitkanant.com/h5#/home, which was not the link to Bitkan, but instead the link to a fake cryptocurrency trading platform.

13. In or around the end of January 2023, after receiving assurances about the safety of the website for investments and the trust K.W. had developed for Jeanie due to their romantic relationship, K.W. agreed to create an account on Bitkanant.com/h5#/home and make some small investments. In total, K.W. invested approximately \$95,000. K.W. transferred money to his cryptocurrency wallets at Cypto.com or Coinbase and then transferred either Bitcoin or Ethereum to what K.W. believed were his wallets at Bitkan. K.W. made some trades on the website based on Jeanie's recommendation from "her uncle" and made significant profits in a short period of time. K.W. was then able to make small withdrawals from what K.W. believed was his Bitkan account. This gave K.W. further comfort in the platform and convinced K.W. to make additional investments. Between February and March 2023, Jeanie manipulated K.W. into investing his entire individual retirement account (IRA), totaling approximately \$1.8 million.

14. When K.W. attempted to withdraw any funds over \$50,000, he received a message that the withdrawal was disallowed unless taxes, fines, and fees were transferred to the website as USDT. K.W. transferred approximately \$669,000, which included a 20% tax, approximately \$516,000 due to a trigger in the system claiming money laundering, \$140,000 for a 5-year VIP

pass, \$100,000 for a blockchain large transfer channel, \$57,000 to return profit the site claimed was an irregular operation, and \$100,000 for an instant withdrawal fee. In total, the purported “taxes, fines, and fees” transferred by K.W. amounted to \$1.6 million.

15. In or around April 2023, Jeanie began having less communication with K.W. The last contact was in July 2023. Soon after communication with Jeanie ended, Bitkanant.com/h5#/home was taken down. In or around August 2023, K.W. located a new website on his own, Bitkancie.com, which was the same exact site as Bitkanant.com/h5#/home and K.W. was even able to log in using the same credentials and see his investments. K.W. subsequently reported the fraud to the FBI Internet Crime Complaint Center on August 3, 2023, leading to the initiation of this investigation.

Tracing of Victim K.W.’s Funds to the **Subject USDT Addresses**

16. Seven of K.W.’s cryptocurrency transactions were traced to the **Subject USDT Addresses**, as detailed below. The traces were conducted using the Last-In-First-Out accounting principle – meaning the most recently deposited items are recorded as the next withdrawal. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

17. The following two transactions made by K.W. were traced to **USDT Address A**:

a. On February 4, 2023, K.W. sent 199,990 USDT from K.W.’s Crypto.com account to address 0x96C93A, which K.W. believed to be with Bitkan. From there, 199,990 USDT was sent to 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address A on March 11, 2023, as part of a 500,000 USDT transaction.

b. On February 6, 2024, K.W. sent 87,990 USDT from K.W.’s Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. From there, 87,990 USDT sent to

0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address A on March 11, 2023, as part of a 500,000 USDT transaction.

c. As of May 8, 2024, when the address was frozen by Tether at FBI request, approximately 499,535 USDT was present in USDT Address A, 287,980 of which can be traced as proceeds directly from K.W.

18. The following transaction made by K.W. was traced to **USDT Address B:**

a. On March 8, 2023, K.W. sent 199,990 USDT from K.W.'s Crypto.com account to address 0x96C93A, which K.W. believed to be with Bitkan. From there, 199,990 USDT was sent to 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address B in eleven installments from March 11, 2023 to March 21, 2023 totaling 243,099 USDT.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 684,279 USDT was present in USDT Address B, 151,708 of which can be traced as proceeds directly from K.W.

19. The following transaction made by K.W. was traced to **USDT Address C:**

a. On April 21, 2023, K.W. sent 199,990 USDT from his Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address C on May 11, 2023 as part of a 500,000 USDT transaction.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,000 USDT was present in USDT Address C, 199,990 of which can be traced as proceeds directly from K.W.

20. The following transaction made by K.W. was traced to **USDT Address D**:

a. On April 22, 2023, K.W. sent approximately 108,141 USDT from his Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address D on May 11, 2023 as part of a 500,000 USDT transaction.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,004 USDT was present in USDT Address D, 108,141 of which can be traced as proceeds directly from K.W.

21. The following two transaction made by K.W. were traced to **USDT Addresses E**:

a. On March 9, 2023, K.W. sent 180,790 USDT from his Crypto.com account to address 0x96C93A which K.W. believed to be with Bitkan. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address E on March 11, 2023 as part of a 500,000 USDT transaction.

b. Also on March 9, 2023, K.W. sent approximately 126.61 ETH from his Coinbase account to address 0x96C93A which K.W. believed to be with Bitkan. The 126.61 ETH was transferred to address 0x7C9702 and converted to 193,745 USDT, using the decentralized exchange Tokenlon. The majority of these funds were transferred to several more addresses, commingled with additional USDT, and ultimately sent to USDT Address E on March 11, 2023 as part of a 500,000 USDT transaction.

c. As of May 8, 2024, when the address was frozen by Tether at FBI request, approximately 499,424 USDT was present in USDT Address E, 294,044 of which can be traced as proceeds directly from K.W.

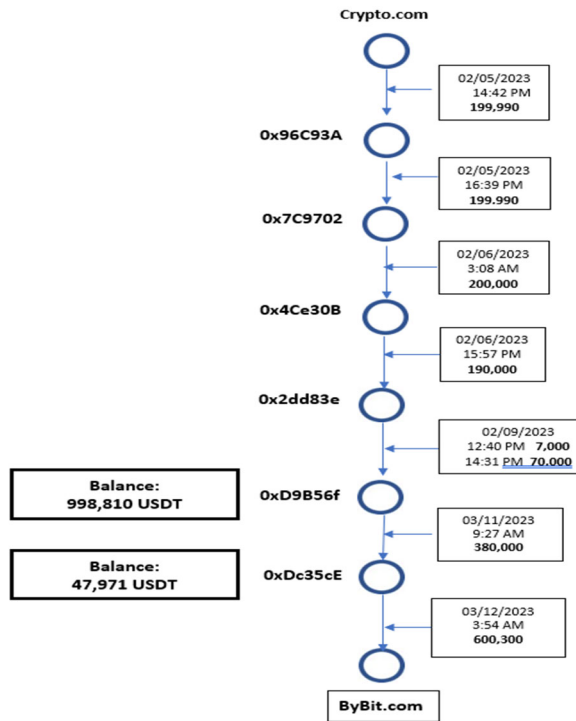
22. In tracing K.W.'s cryptocurrency transactions, agents determined that two addresses (**USDT Address H** and **USDT Address I**) had funds remaining after the pass-through transfer of K.W.'s funds. Through the analysis described below, Addresses H and I were used for the purposes of commingling the proceeds of the fraud with other USDT² in furtherance of laundering the proceeds. Specifically:

a. On February 5, 2023, K.W. sent approximately 199,990 USDT from his Crypto.com account to address 0x96C93A, which K.W. believed to be with Bitkan. These funds were commingled with additional USDT, transferred through several more addresses, including USDT Address H (0xD9B56f) and USDT Address I (0xDc35cE), and ultimately sent to an address at the exchange Bybit.com on March 12, 2023 as part of a 600,300 USDT transaction.

b. As of May 8, 2024, when the address was frozen by Tether at FBI request, approximately 998,810 USDT was present in USDT Address H, and 47,971 USDT was present in USDT Address I.

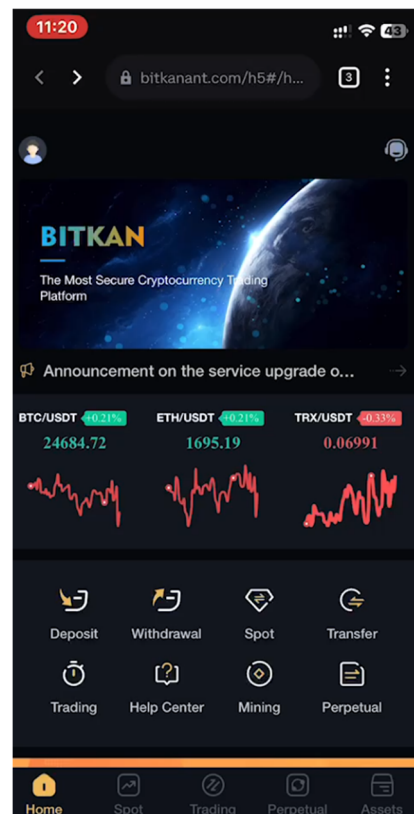
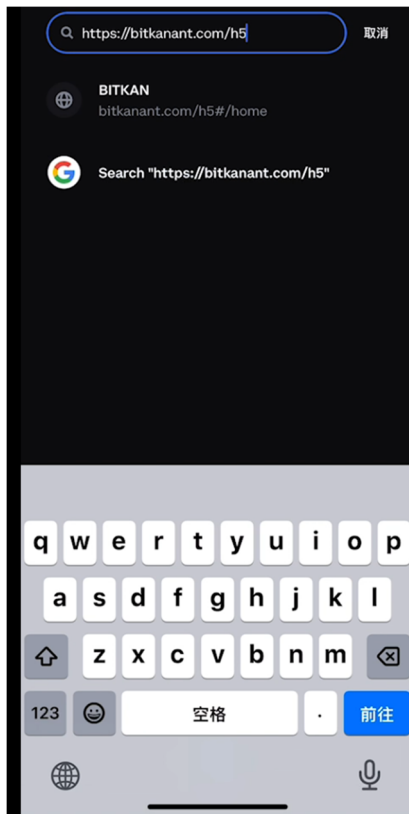
c. The following is a graphical representation of these transactions:

² Analysis of the addresses H & I indicates other deposits into the address were also fraudulent proceeds.



Victim J.B.

23. J.B. is an 83-year-old resident of Bayfield, Minnesota. In February 2023 a person claiming to be a woman named Alice contacted J.B. via text message, said she received his phone number from another person, and that she wanted to verify it was really them. They later communicated via WhatsApp and Telegram. Alice (who later said her real name was Jengyi Lee) said she worked in fashion design in Miami, Florida. Alice also claimed to be from Hong Kong. J.B. and Alice eventually discussed cryptocurrency. J.B. said he had lost money on his investment in BTC and ETH, but he still held various cryptocurrencies in Coinbase. Alice introduced J.B. to what J.B. believed was a cryptocurrency trading platform called Bitkan. However, Alice deceived him into creating an account at a fraudulent site, Bitkanant, by providing the website address as “Bitkanant.com/h5#/home” rather than the true website address, Bitkan.com. Screenshots included below demonstrate how Alice deceived J.B. into accessing the fraudulent website rather than the legitimate Bitkan website.



24. In or around the middle of February 2023, J.B. transferred money to his wallets at Coinbase and then transfer either USDT or ETH to what J.B. believed were his wallets at Bitkan. J.B. made some trades on the website based on Alice's recommendation from her uncle and, according to Bitkan, made significant profit in a short period of time. Between February and April 2023, Alice manipulated J.B. into investing all of his savings, including a surrendered life insurance policy, totaling approximately \$950,000.

25. In or around May 30, 2023, after Adult Protective Services was contacted by J.B.'s bank, the Bayfield County Sheriff's Office filed a fraud report to the FBI Internet Crime Complaint Center (IC3) on J.B.'s behalf. J.B. and the Bayfield County Sheriff's Office attempted to withdraw money from J.B.'s Bitkan account but were unsuccessful.

Tracing of Victim J.B.'s Funds to the **Subject USDT Addresses**

26. Two of J.B.'s cryptocurrency transactions were traced to the **Subject USDT Addresses**, as detailed below. The traces were conducted using the Last-In-First-Out accounting principle – meaning the most recently deposited items are recorded as the next withdrawal. For clarity, all cryptocurrency addresses have been shortened to the first eight characters.

27. The following transaction made by J.B. was traced to **USDT Address F**:

a. On March 9, 2023, J.B. sent 13.59 BTC from J.B.'s Coinbase.com account to address 3HvFNTok which J.B. believed to be with Bitkan. From there, the funds were converted to 268,865 USDT via Tokenlon and deposited at address 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address F on May 11, 2023, as part of a 500,000 USDT transaction.

b. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,004 USDT was present in USDT Address F, 268,865 of which can be traced as proceeds directly from J.B.

28. The following transaction made by J.B. was traced to **USDT Address G**:

c. On April 14, 2023, J.B. sent 9.02 BTC from J.B.'s Coinbase.com account to address 07x788EB which J.B. believed to be with Bitkan. From there, the funds were converted to 18,896.26 USDT via Tokenlon and deposited at address 0x7C9702. These funds were commingled with additional USDT, transferred through several more addresses, and ultimately sent to USDT Address G on May 11, 2023 as part of a 500,000 USDT transaction.

d. As of April 16, 2024, when the address was frozen by Tether at FBI request, approximately 500,004 USDT was present in USDT Address G, 18,896.26 of which can be traced as proceeds directly from J.B.

Tracing of Other Probable Victims' Funds to the **Subject USDT Addresses**

29. There are several factors which indicate that the two victims described above are part of the same larger fraud scheme. These factors show that the **Subject USDT Addresses** have been used not only to launder the proceeds of criminal activity received from K.W. and J.B., but from numerous other victims who are unknown at this time.

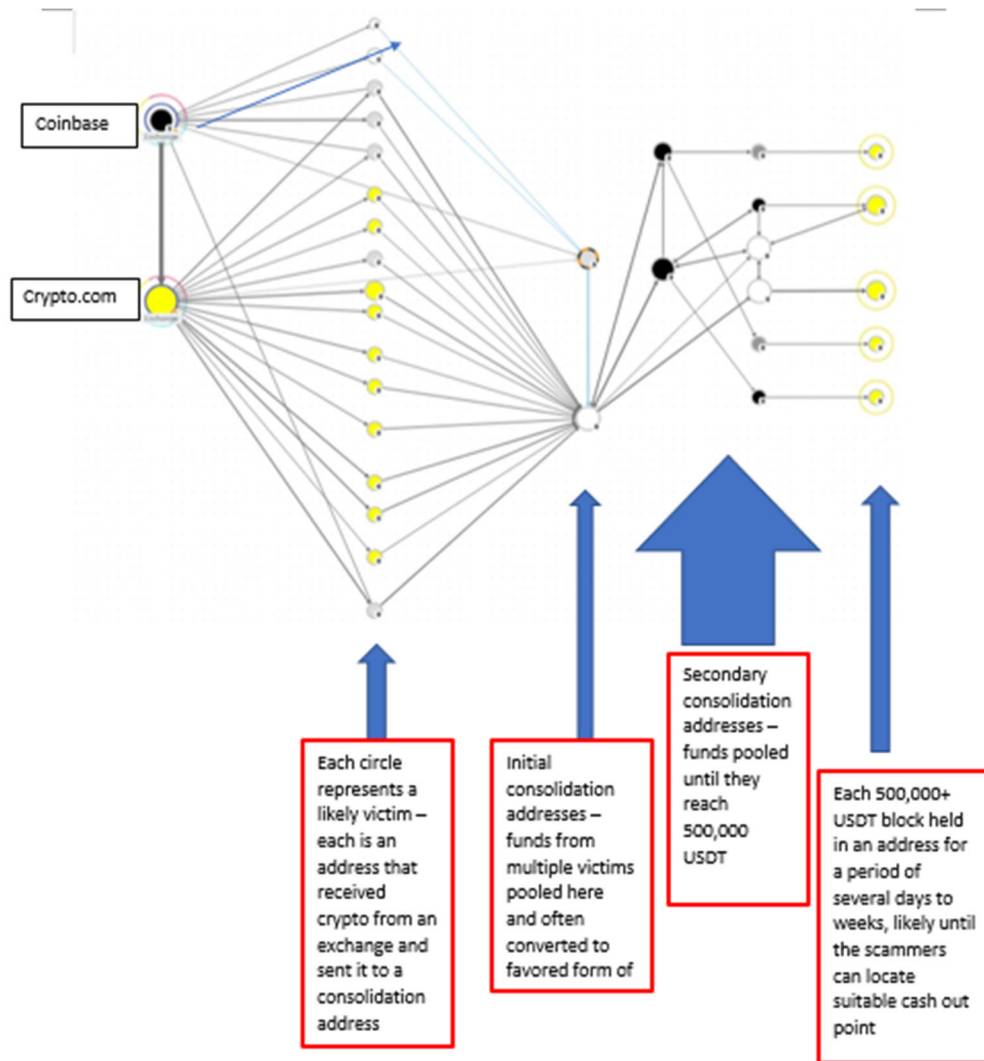
a. *Shared cryptocurrency addresses and patterns of activity:* In cryptocurrency investment fraud schemes, victims are often given individual “burner” cryptocurrency addresses which are provided only to that particular victim. When a victim sends cryptocurrency to the burner address, the cryptocurrency is then quickly sent to another address where funds from multiple victims are consolidated. There are often multiple layers of consolidation addresses, which can be seen in this case. Specifically:

i. The tracing of victim transactions in this case showed that all of the transactions which led to Subject Addresses A, B, C, D, and E were sent through consolidation addresses, 0x96C93A and 0x7C9702. Transactions which led to USDT Address F and USDT Address G were sent through other addresses before passing through consolidation address 0x7C9702. USDT Address E and USDT Address F also shared consolidation address 0x02b725, and USDT Address C and USDT Address F shared consolidation address 0x1345ef.

ii. In sum, based on my training, experience, and the investigation to date, I believe that each victim transaction shows a common pattern of moving to an initial consolidation address, where it is converted to what appears to be the scammers' favored form of cryptocurrency, USDT. The USDT is then sent to a secondary consolidation address, where it is further comingled or transferred to several more addresses, then parceled out into addresses often containing approximately 500,000

USDT each. This was the common pattern for the transactions conducted on funds originating from K.W. and J.B.

b. The chart below was created by “backtracing” from the consolidation addresses that had been identified when tracing K.W. and J.B.’s transactions. In backtracing, instead of tracing forward to find out where the funds were sent, transactions were traced backward to see what other addresses had sent funds to the consolidation addresses, and where those funds originated from, which in every case was an exchange. In my experience this technique is very successful in locating additional victims who may not have reported the scam or may not yet be aware they are a victim.



c. *Other Victim Reporting:* A search of the FBI’s IC3 identified 71 other potential victims of this scam. These victims were located by searching for and “Bitturk” and “Bitkan” in the database. Each of these victims reported a similar scam to those detailed here, with some variations in how they were recruited for the scam, the name the scammer used when contacting the victim, and the specific URL used to access the platform.

30. During the freeze period and prior to the service of the seizure warrant, two potential claimants came forward and contacted Tether for wallet address 0xDc35cE037722e2196a8B3eB9da64648Bc0E037C8. The first claim was made on May 17, 2024


by an individual who provided the name Chen Fui Fong, however Fong elected not be interviewed by the FBI. The second claimant identified themselves as Zheng Lee and contacted Tether on June 13, 2024. Lee was interviewed by the FBI on June 25, 2024. During the interview, Lee stated he bought and sold USDT on behalf of others and did not always know with whom he was doing business. Lee also claimed he could purchase USDT for a lower price than the Tether platform as he was purchasing USDT using Malaysian money. Lee provided no legitimate explanation for the activity in this wallet. As unhosted Tether wallets are anonymous, it was not possible to obtain any ownership information on this wallet or any of the other eight wallets seized.

CONCLUSION

31. Based on information derived from the foregoing investigation, there is probable cause to conclude that the **Subject USDT Addresses** received and contain the proceeds of a wire fraud scheme in violation of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy to commit wire fraud). Those proceeds are subject to seizure and forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C). In addition, there is probable cause to believe that the contents of the **Subject USDT Addresses** constitute property involved in money laundering transactions in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 1956(h) (money laundering and conspiracy to commit money laundering), and are therefore subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A).

32. The foregoing facts are furthermore sufficient to support a reasonable belief that the defendant property is forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) and/or 18 U.S.C. 981(a)(1)(A).

Executed this 8th day of November, 2024.



David Harding
Special Agent
Federal Bureau of Investigation